

Fig. 1

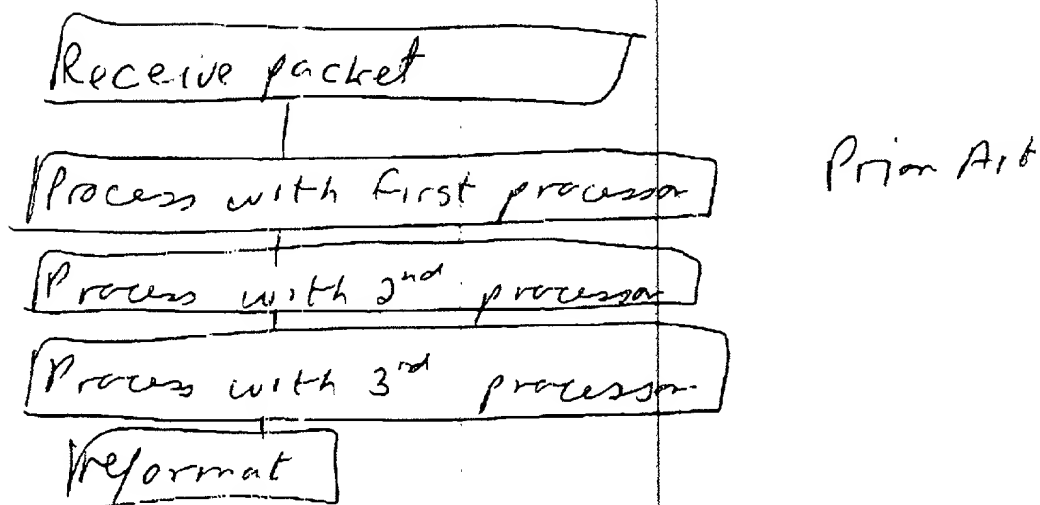


Fig 2

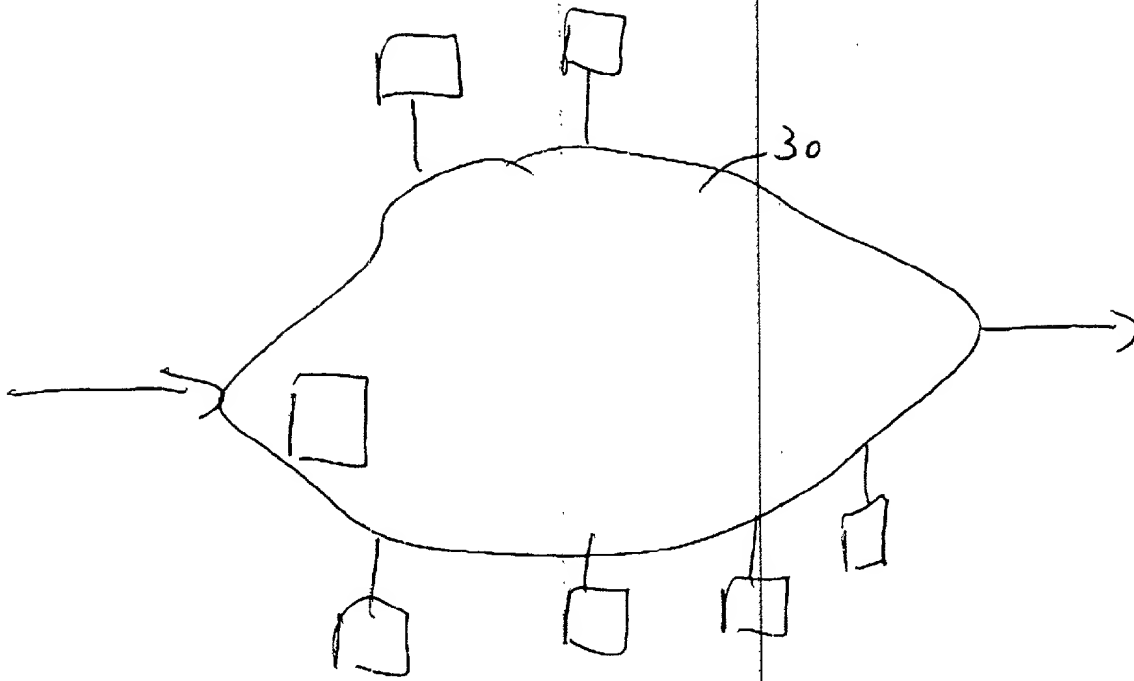


Fig. 3

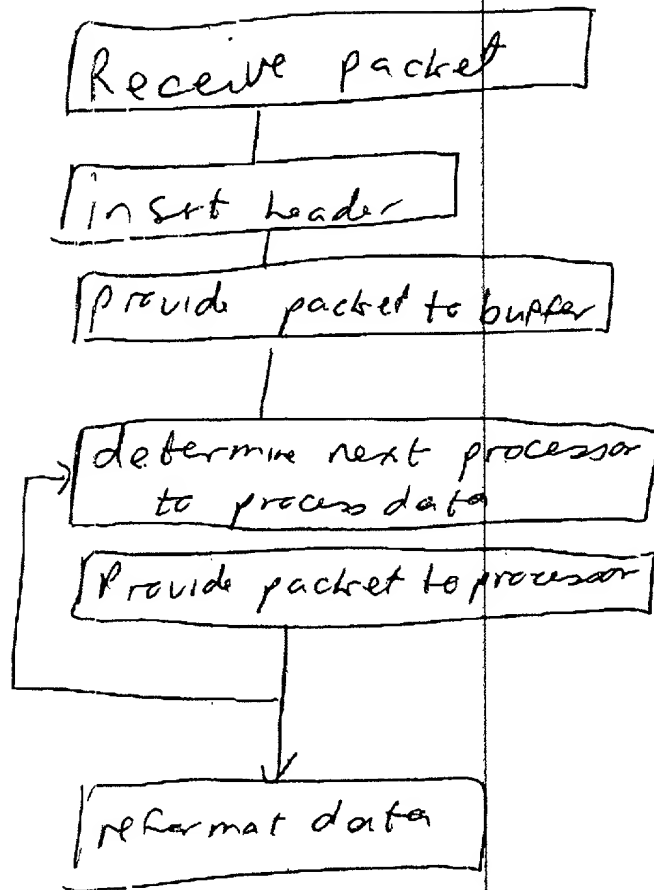


Fig. 4

418035 PROMOTING NEXT GENERATION NETWORK SECURITY

**Chrysalis-ITS Confidential**

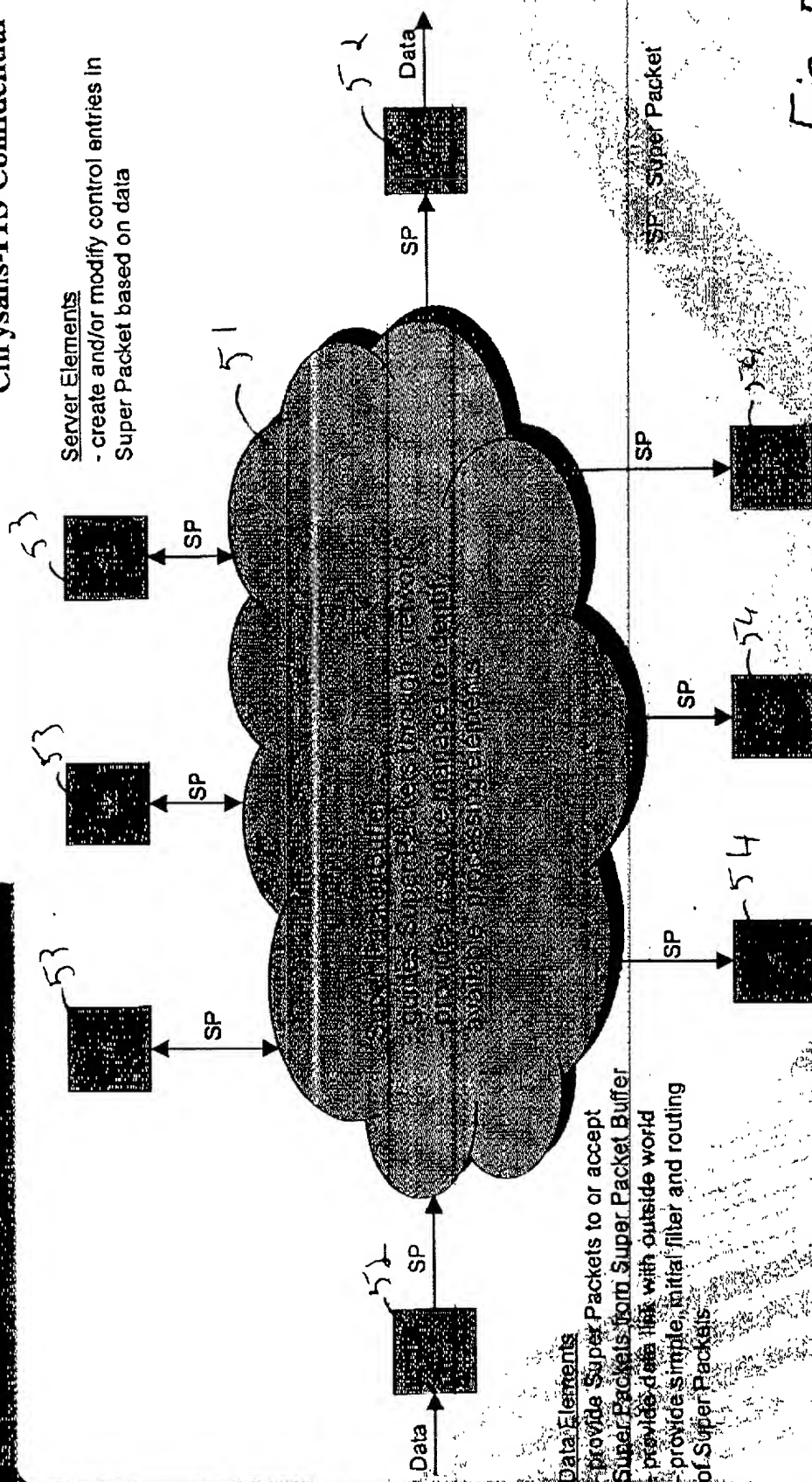


Fig. 5

## Client Elements

- Packet Functions**
- perform simple processing functions on data as specified in Super Packet control
  - can modify data and associated control entries in the Super Packet
  - can not add or subtract control entries from Super Packet

## Generic Processing Element

- can interact with a super packet and super packet buffer
- can modify control and data elements of super packet

Copyright 1999-2000, Chrysalis-ITS, Inc. All rights reserved.

27 November 2000

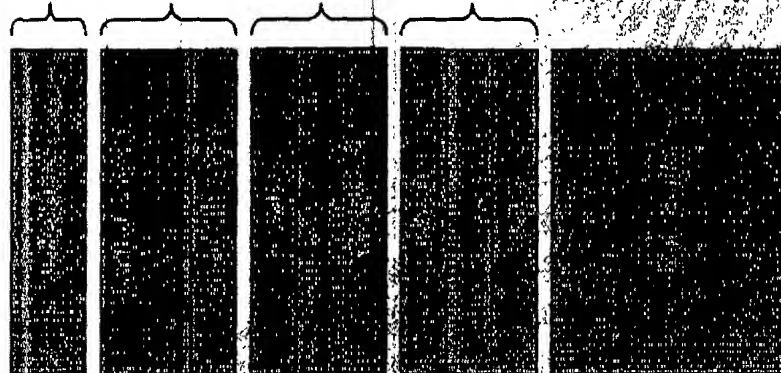
30

## EMPOWERING NEXT GENERATION NETWORK SECURITY

Chrysalis-ITS Confidential

# Super Packet

- Contains all control, coding, keying information required to process the contained data



Data buffer controls original and modified data.

Fig 6



27 November 2000

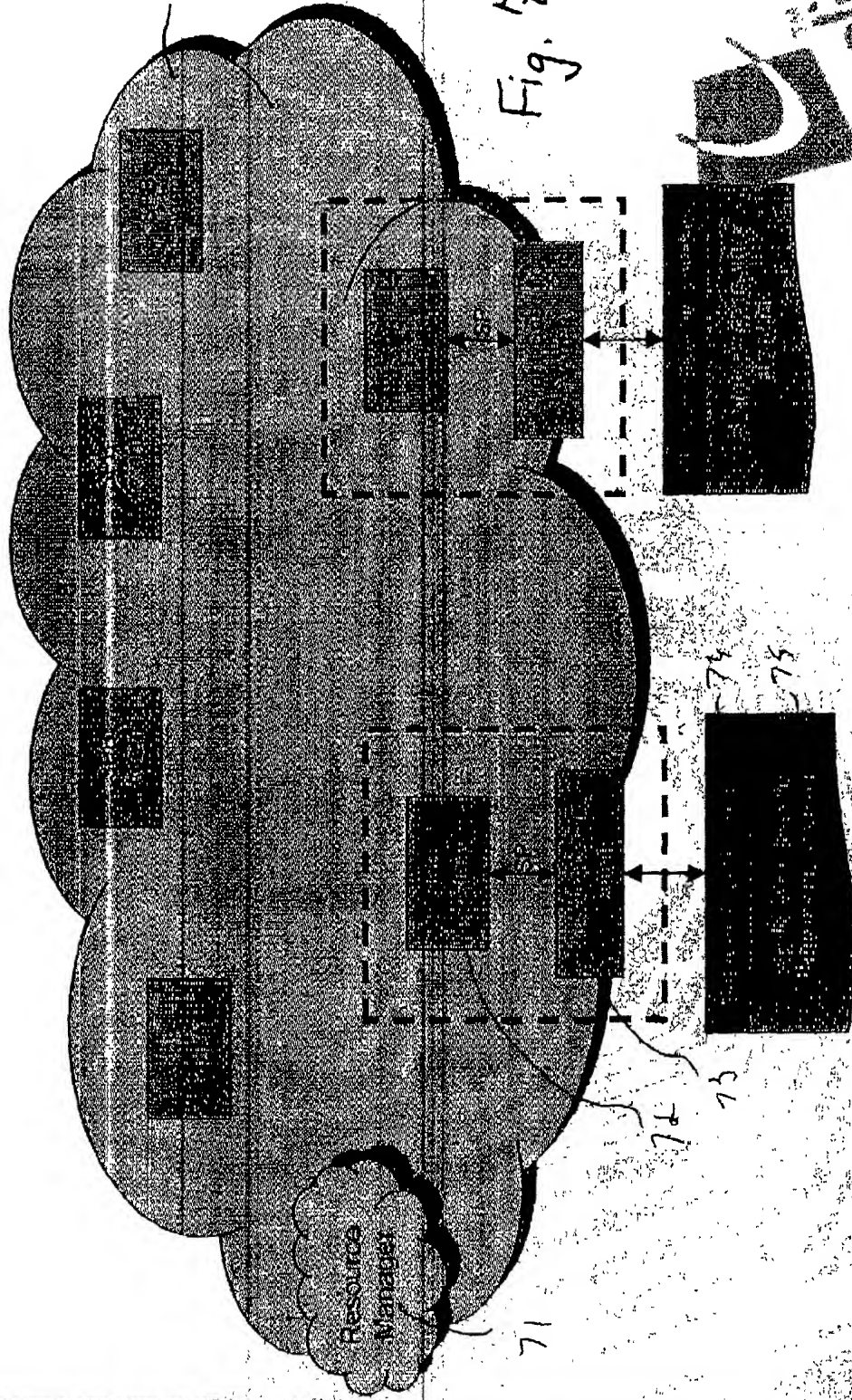
Copyright 1999-2000, Chrysalis-ITS, Inc. All rights reserved.

# EMPOWERING NEXT GENERATION NETWORK SECURITY

Chrysalis-ITS Confidential

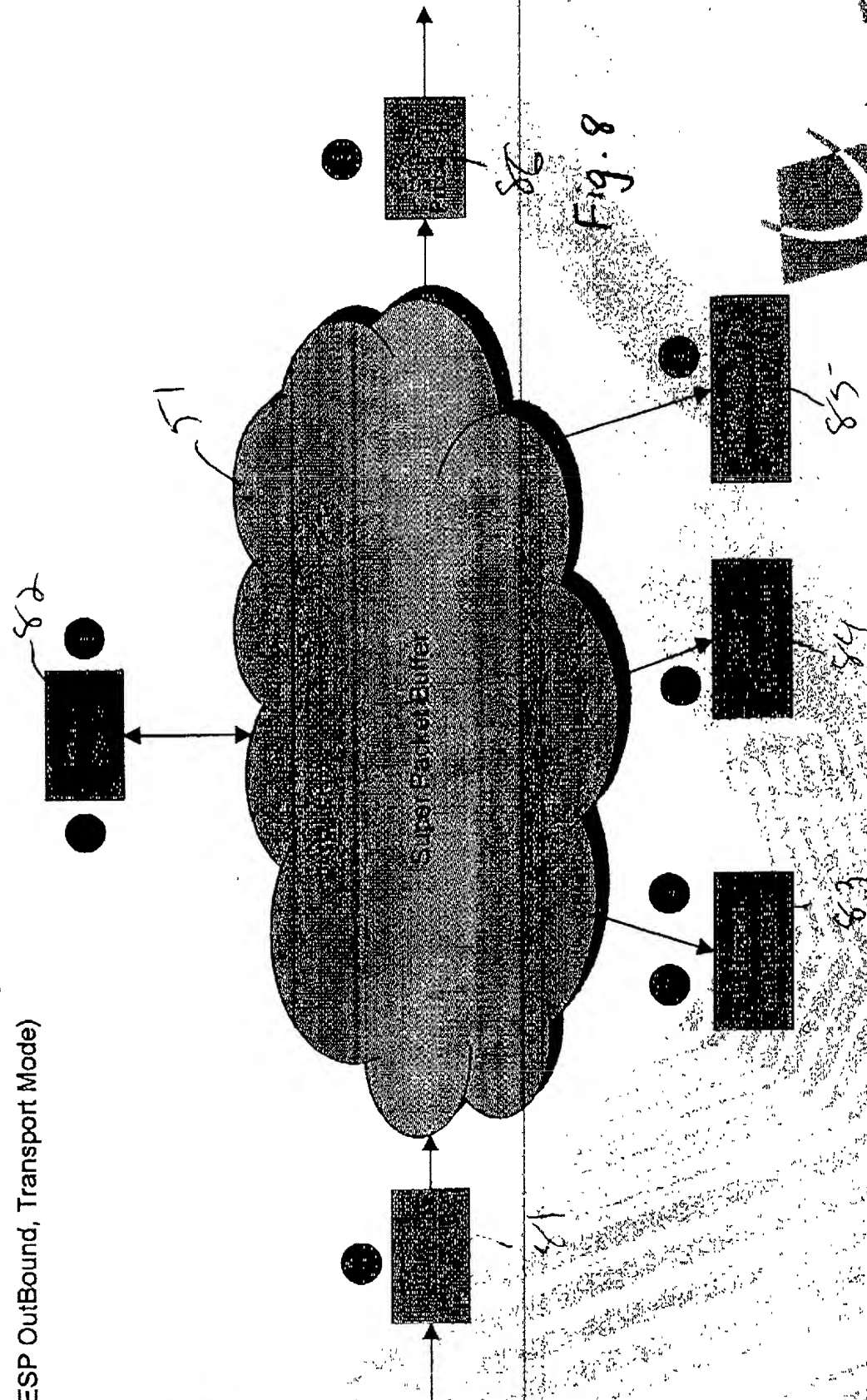
## Super Packet Buffer

- Responsible for moving Super Packet between the generic processing elements



# IPSec Processing Example

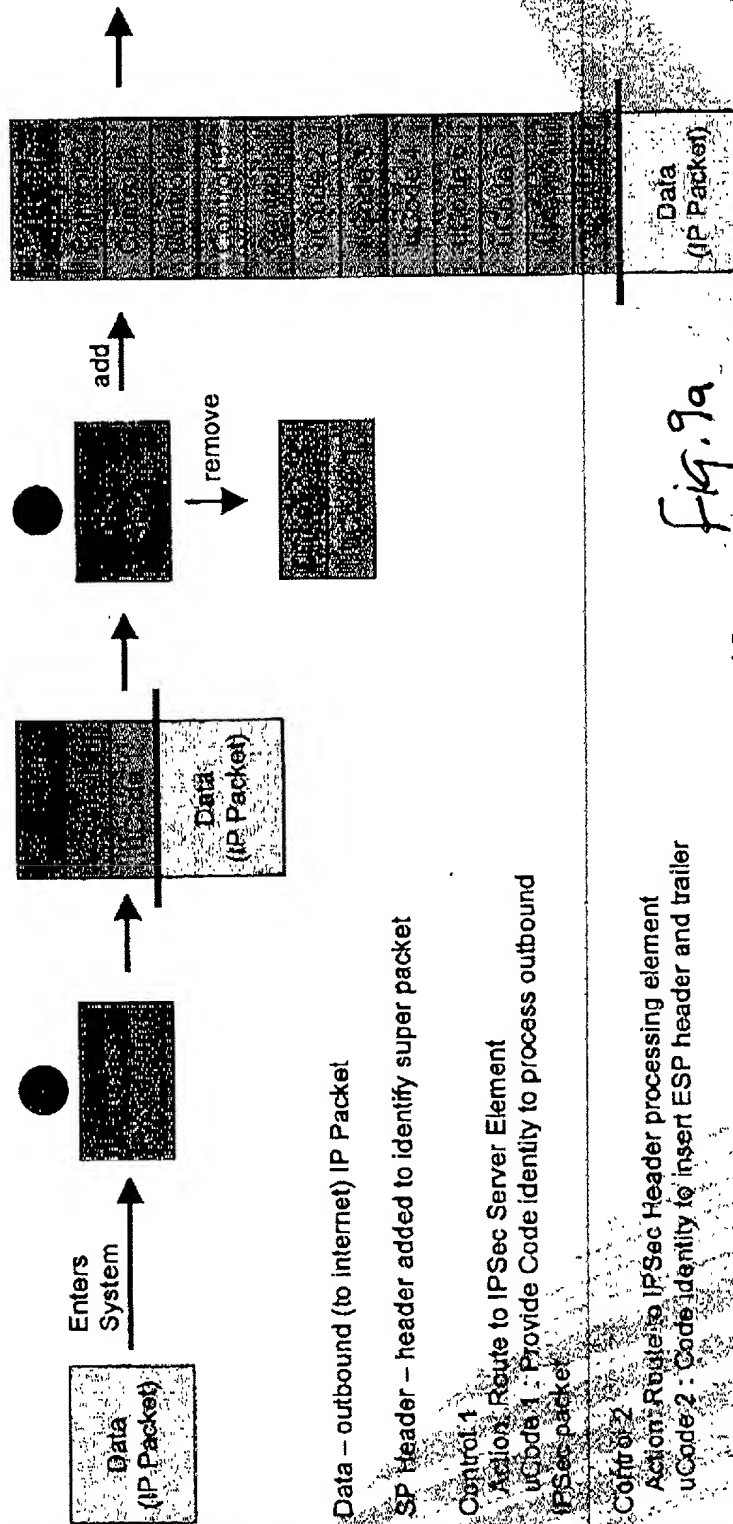
(ESP OutBound, Transport Mode)





Chrysalis-ITS Confidential

# IPSec Super Packet (1)



Data – outbound (to Internet) IP Packet

SP Header – header added to identify super packet

Control 1

Action: Route to IPSec Server Element

uCode 1: Provide Code Identity to process outbound

IPSec packet

Control 2

Action: Route to IPSec Header processing element

uCode 2: Code identity to insert ESP header and trailer

Control 3

Action: Route to 3DES processing element and encrypt

uCode 3: 3DES algorithm (CBC Mode)

Key 3: 3DES key for packet

Control 4

Action: Route to HMAC96-MD5 processing element and

generate MAC

uCode 4: HMAC96-MD5 algorithm

Key 4: HMAC Key for packet

Control 5

Action: Place MAC in ESP Header

uCode 5: Code identity for post encryption header

manipulation

Control 6

Action: Route to Egress Unit

uCode 6: Code identity to strip new IP Packet from

Packet and transmit

Fig. 9a

27 November 2000

Copyright 1999-2000, Chrysalis-ITS, Inc. All rights reserved.





THIS DOCUMENT CONTAINS INFORMATION THAT IS UNCLASSIFIED

EXCEPT WHERE SHOWN OTHERWISE BY A CROSS-HATCH

Chrysalis-ITS Confidential

## IPSec Super Packet (2)

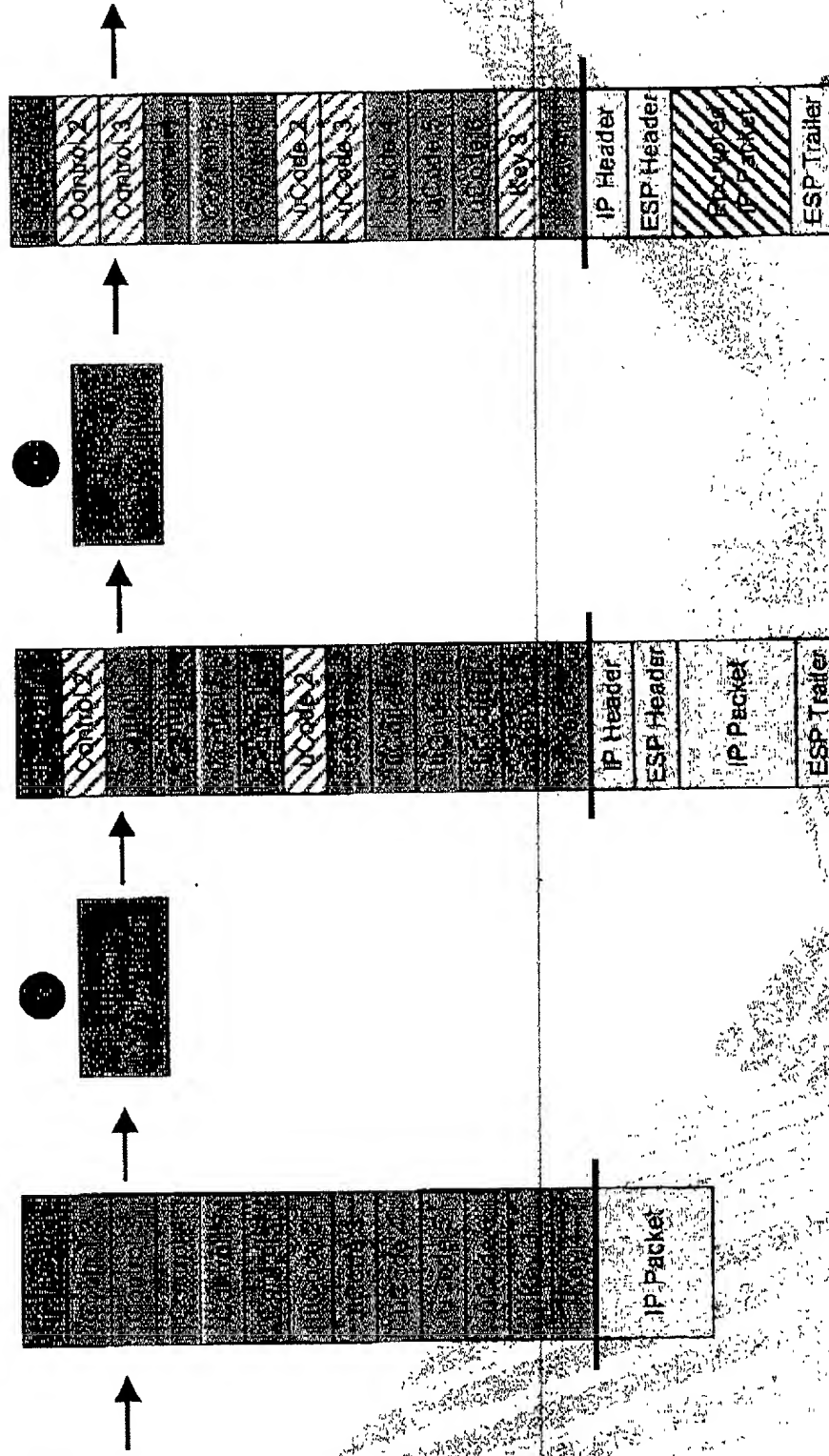


Fig. 9b

Cross hatch indicates processing complete.



## IPSec Super Packet (3)

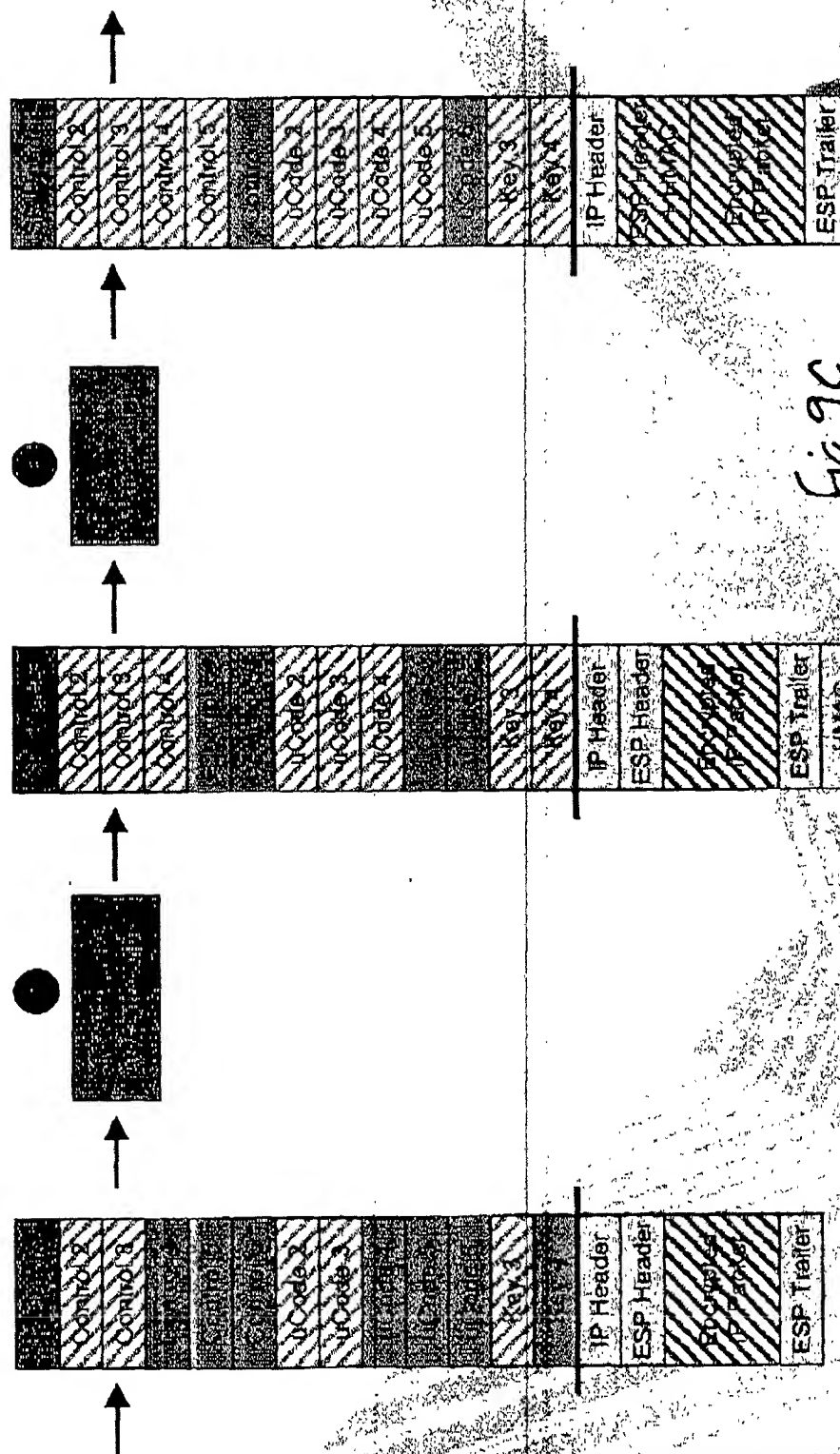


Fig. 9C

Cross hatch indicates processing complete

# IPSec Super Packet (4)

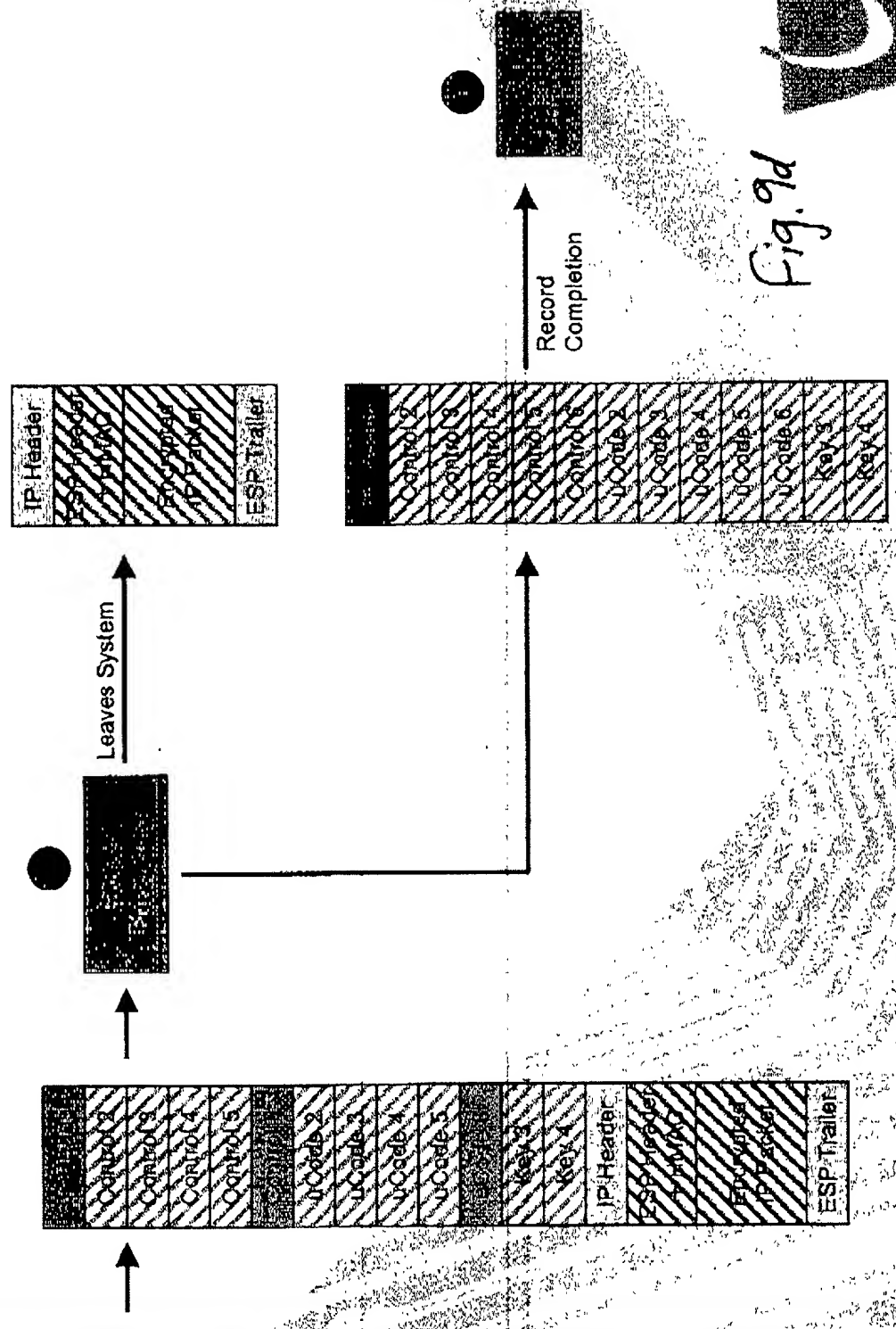
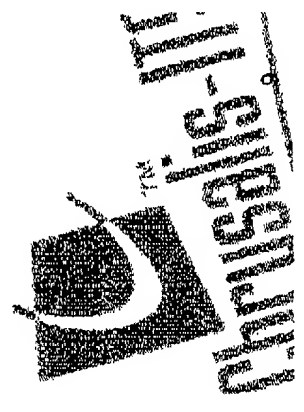


Fig. 9d

Cross hatch indicates processing complete



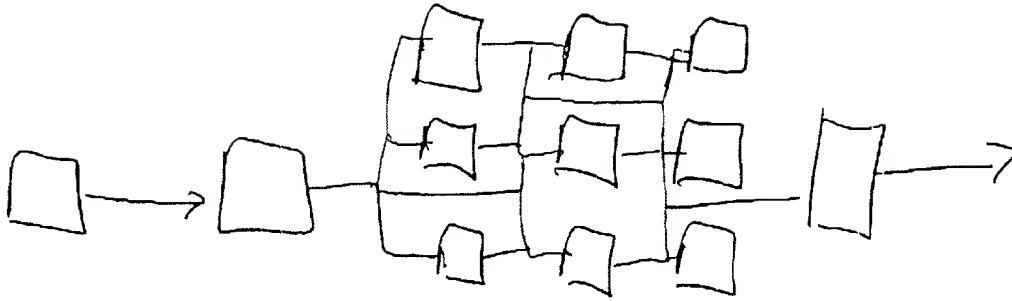


Fig-10